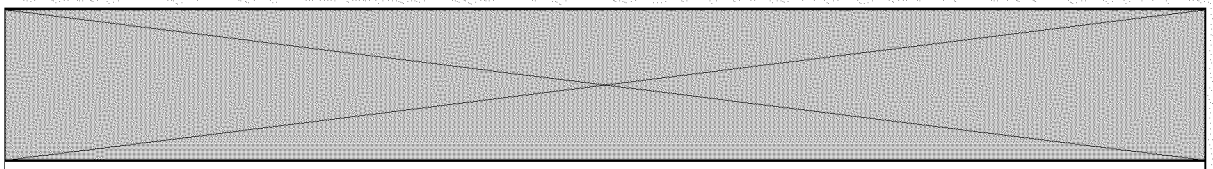
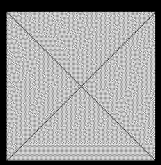
To: Flynn, Mike[Flynn.Mike@epa.gov]
From: GovernmentCIO Journal
Sent: Tue 6/13/2017 2:50:35 PM
Subject: GovernmentCIO Journal Weekly Newsletter

Is this email not displaying correctly?
View it in your browser.



Inside the FDA's IT Strategic Plan

When the U.S. Food and Drug Administration released its IT Strategic Plan in September 2015, Chief Information Officer Todd Simpson incorporated a review process in order to revisit the plan annually and ensure it keeps up with mandates, new technologies and priorities.



SUBSCRIBE NO\

FORWARD

Congressman Jim Langevin's Three Cybersecurity Priorities

ities in a world of machine cted devices

Congressman Jim Langevin (D-RI), ranking member of the Subcommittee on Emerging Threats and Capabilities, identified a leading problem facing national cybersecurity today: as technology continues to improve, the networks that need to be protected are only becoming more complicated.

Speaking at the Institute for Critical Infrastructure Technology (ICIT) Forum on June 7 in Washington, D.C., Langevin explained that traditionally, patching vulnerabilities typically involves modifying software with some code changes. Yet when the vulnerability is a trained, machine-learning behavior, how does it get patched? (More...)

Patching National Cybersecurity Threats Starts with Supply Chain

The national cybersecurity threat level is evolving, and government officials are calling on industry to better secure the Internet of Things and connected devices as they continue to enter government networks.

Deloitte's Seven Emerging Tech Trends

The company found the next phase of IT innovation facing CIOs in and out of government

In Deloitte Consulting LLP's recently released tech trends report, "The Kinetic Enterprise," it identified the forces that remain constant in driving IT transformation; digital, analytics, cloud, the reimagining of core systems... (More...)

Tech Corner

Automate Table Auditing

The National Institute of Standards and Technology (NIST) establish the security

audit policies, content and availability of audit results in the event of software changes. Specifically, AU-2 (Audit Events), AU-3 (Content of Audit Records) and AU-12 (Audit Generation) address when an audit is required, what is included in the audit and the ability to generate audit records. The remaining controls in this family provide the guidance for ensuring that the system is capable of storing and protecting the audit records, that they are accessible and that they are able to be analyzed by the appropriate personnel.